统一用户目录管理

统一用户目录管理是为了方便用户访问组织机构内所有的授权资源和服务，简化用户管理，基于 LDAP 或基于数据库，对组织机构内中所有应用实行统一的用户信息的存储、认证和管理。

统一用户目录管理要遵循以下两个基本原则：

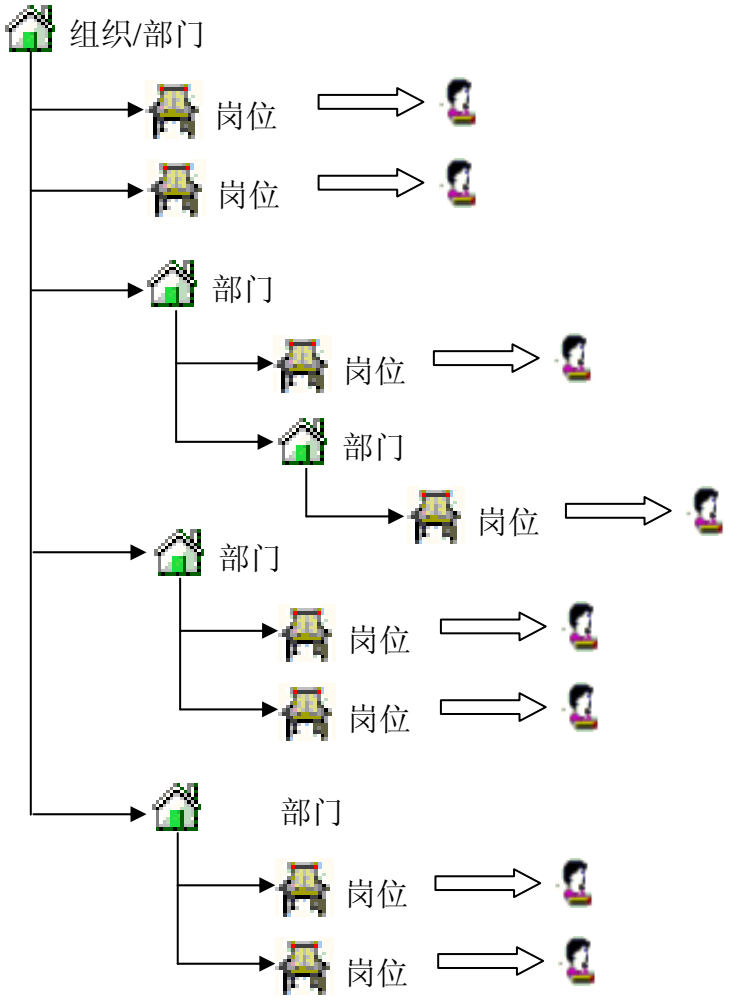
- **统一性原则**：实现对目前已知用户类型进行统一管理；对包括分支机构在内的整个组织机构内的所有用户进行用户目录复制和统一管理；对门户的用户体系和各应用系统各自独立的用户体系进行统一管理；对新进员工/用户到员工/用户离开进行整个生命周期的管理。
- **可扩充性原则**：能够适应对将来扩充子系统的用户进行管理。

1.1 用户分类模型

1.1.1 基于部门岗位树的角色模型

基于部门岗位树的角色模型是组织机构内最常见的模型，提供了用户目录管理、目录复制、权限控制的多种属性。角色管理是用户权限管理的重要基础。

基于部门岗位树的角色模型如下所示：



在部门岗位角色树状层次模型中，用户职位称为岗位，或称用户角色，包含岗位角色的组织机构称为部门，大部门可以包含小部门。其最重要的特点是：

- 用户隶属于岗位/角色(可以隶属于多个岗位/角色)；
- 岗位/角色具有时间范围；
- 部门包含下属部门及岗位/角色中的所有用户。

部门岗位角色树状层次模型，比如：

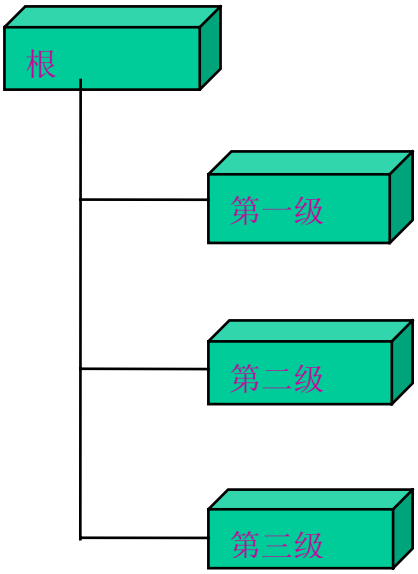
- 如集团、总部/华北/华东/华南等大区、分支机构、部门、科室等；
- 如国家部委、省级/地市等分支机构、司/局、处、科室等；
- 再如学校、分校、学院、研究室/班级、教师/职工/家属/学生等。

用户信息以组织/部门/岗位角色以树状的层次结构来组织和管理，有以下好处：

- 同实际组织机构体系相一致；
- 同 LDAP 目录对数据的组织方式保持一致，便于利用 LDAP 目录服务的强大进行用户目录的管理；
- 有利于将某个地域/分支机构或某个部门/下属单位的用户信息定制推送到单独的用户目录服务器上，提高相关应用对用户信息的访问效率；
- 有利于根据目录树的结构给予不同的员工/用户组不同的权限。

1.1.2 级别分层树模型

级别分层树模型如下图所示，是对部门岗位角色树状层次模型的补充。



在级别分层树模型中，不同层次的节点具有上下级或涵盖关系。相同层次的节点相互独立，之间没有上下级或涵盖关系。

其最重要的特点是：

- 用户只能属于一个级别；
- 在同一层次节点下可以有多个级别；
- 可用大于、小于或等于，以上、以下等词汇来指定多个或一个层次的级别。

级别分层树模型，比如：

- 市长、副市长、委办局长、副局长、处长/副处长、科长等行政级别；

- 部委部长/主任、司局长/厅长、处长/副处长、科长等行政级别；
- 公司总裁/总经理、副总裁/副总经理、部门总监/部门经理/部长、高级经理、项目经理、普通员工等级别；
- 校长、副校长、院长、副院长、博导/教授、副教授、讲师；学生：博士研究生、硕士研究生、本科生等级别。。。

利用级别分层树模型，可辅助实现更为灵活的用户授权控制。

1.2 用户信息存储管理

1.2.1 用户信息存储分类

统一的用户信息存储可基于：

- **数据库方式**：支持将统一的用户信息存储于各大主流数据库中，如 Oracle、DB2、SQL Server、Sybase、MySQL 等；
- **LDAP 目录方式**：支持将统一的用户信息存储于 LDAP 目录中，如 Domino LDAP、Sun One Directory Server、OpenLDAP、MS Active Directory、Novell NDS、Netscape Directory Server 等。

此外，可以**基于 LDAP 目录或数据库方式，新建一个用户信息目录库**，供门户和应用系统使用；

也支持可以**使用现存应用系统的已有用户数据库**，作为门户和其他应用统一的用户信息存储管理库，如可以考虑基于现存的 OA 办公自动化系统、或者 HR 人事系统、或者一卡通系统等现有系统的 RDBMS 用户数据库或 LDAP 用户目录进行用户信息管理和身份验证。

鉴于基于 LDAP 目录服务存储和管理用户的身份认证等信息，可更有效更灵活地管理用户及资源，**我们推荐采用 LDAP 目录服务作为各组织机构信息化建设统一用户管理的基础平台**。下面主要阐述 LDAP 目录服务的相关内容。

1.2.2 LDAP 目录服务定义

LDAP 协议： 轻量级目录访问协议(LDAP)，英文全称是 Lightweight Directory Access Protocol，是一个用于访问存储在信息目录中的信息的 Internet 协议，是目录服务在 TCP/IP 上的实现（RFC 1777 V2 版和 RFC 2251 V3 版）。它是对 X500 的目录协议的移植，但是简化了实现方法，所以称为轻量级的目录服务。

LDAP 协议是跨平台的和标准的协议；实际上，LDAP 作为一种 Internet 标准，得到了业界的广泛认可。

LDAP 的核心规范在 RFC 中进行了定义，LDAP 协议集规定了区别名(DN)的命名方法、存取控制方法、搜索格式、复制方法、URL 格式、开发接口等，描述了客户端应该如何访问存储在服务器上的数据，但没有定义应该如何存储数据。通过使用 LDAP，可以在信息目录的正确位置读取（或存储）数据。

目录服务：所谓**目录服务**是在分布式计算机环境中，定位和标识用户以及可用的各网络元素和网络资源，并提供搜索功能和权限管理功能的服务机制。各组织机构为了实现各个分立的“信息孤岛”走向连通和融合，一方面业务系统需要将自身的职能和业务协作要求公布出去；另一方面，也希望能够检索并获取其他业务系统的信息和公共的信息资源。这些需求采用目录服务都能够得到满足。

目录服务是其对象具有属性及名称的命名服务，是命名服务的自然扩展。目录服务与命名服务的关键区别在于，目录服务允许属性（比如用户的电子邮件地址）与对象相关联。

目录服务的核心是一个树状结构的信息目录，由一系列具有属性和名称的目录入口对象(Entry)组成，将网络中的数据资源、数据处理资源和用户信息按有次序的结构进行组织，并且专门针对海量查询的使用情况进行了优化，极大地提高了数据读取和查询性能。

目录服务不仅可以提供分布式计算网络的视图，以逻辑的观念来管理网络，而且它能实现以人为本的网络管理方式。它可以记载网络的所有文件以及所有在网络上运行的资源，以及使用者帐号、身份口令、密码、卷、文档，应用程序以

至于域名服务器 DHCP、IP 地址以及认证的公钥等。此外，目录软件还保存和管理对包括人员、业务过程和供内部使用的资源等有关组织机构详细信息的访问。

目录服务树中的一个目录对象可以通过它的名字检索，或者通过使用一组搜索标准（表示目录对象的名字和属性）检索。

在分布式计算环境中，各单位对其他单位有用的信息可以在目录服务注册、解除注册和查询。

在整个组织机构范围内部署和实现 LDAP，可以让运行在几乎所有计算机平台上的所有的应用程序从 LDAP 目录中获取信息。

目录服务与数据库服务的异同：

正如 Oracle、DB2、SQL Server、Sybase 等数据库管理系统是用于处理查询和更新关系型数据库那样，**LDAP 服务器**也是用来处理查询和更新 LDAP 目录的。换句话来说 LDAP 目录也是一种类型的数据库，但是不是关系型数据库。

目录服务与数据库服务的不同之处在于， LDAP 目录服务一般缺少数据库提供的事务功能和大规模数据的数据库支持； 但专门针对读密集型的操作进行了专门的优化，因此，可极大地提高**数据读取和查询性能**；LDAP 把数据存放在文件中，为提高效率可以使用基于索引的文件数据库，而不是关系数据库；LDAP 的数据类型主要是字符型，为了检索的需要添加了 BIN（二进制数据）、CIS（忽略大小写）、CES（大小写敏感）、TEL（电话型）等语法（Syntax），而不是关系数据库提供的整数、浮点数、日期、货币等类型，同样也不提供象关系数据库中普遍包含的大量的函数，它主要面向数据的查询服务（查询和修改操作比一般是大于 10:1），不提供事务的回滚（rollback）机制，它的数据修改使用简单的锁定机制实现 All-or-Nothing，它的目标是快速响应和大容量查询并且提供多目录服务器的信息复制功能；一般而言，当从 LDAP 服务器中读取数据的时候会比从专门为 OLTP 优化的关系型数据库中读取数据快一个数量级。

正是因为专门为读的性能进行优化，大多数的 LDAP 目录服务器并不适合存储需要经常改变的数据；而是若符合以下条件的数据，则比较适合在 LDAP

目录中进行存储。

- **数据需要从不同的地点读取，但是不需要经常更新**。
- 需要在任何平台上都能读取数据；
- 数据为平面数据(Flat Data)，数据记录对象的组织只是为了方便检索和灵活性的需要，LDAP 中属性类型 Type 可以有多个属性值 Value，如员工/用户信息记录可以包含主管领导的登录名； 而不是象关系数据库那样，为降低数据的冗余性要求实现各个域必须是不相关的。

LDAP 目录的优势：

现在 LDAP 的流行是很多因素共同作用的结果。LDAP 的优势主要体现在：

- **跨平台**：可以在任何计算机平台上，用很容易获得的而且数目不断增加的 LDAP 的客户端程序访问 LDAP 目录；而且也很容易定制应用程序为它加上 LDAP 的支持。

  在组织机构范围内实现和部署 LDAP，可以让运行在几乎所有计算机平台上的所有的应用程序从 LDAP 目录中获取信息；而数据源可以放在任何地方，可以方便用户信息系统的集成，简化员工在机构单位内部查询信息的步骤。

  LDAP 协议是跨平台的和标准的协议，得到了业界的广泛认可，因此应用程序就不需关心 LDAP 目录放在什么样的服务器上。软件厂商在产品中加入对 LDAP 的支持，根本不用考虑另一端（客户端或服务端）是怎么样的。LDAP 服务器可以是任何一个开发源代码或商用的 LDAP 目录服务器（或者还可能是具有 LDAP 界面的关系型数据库），因为可以用同样的协议、客户端连接软件包和查询命令与 LDAP 服务器进行交互。与 LDAP 不同的是，如果软件厂商想在软件产品中集成对 DBMS 的支持，那么通常都要对每一个数据库服务器单独定制。
- **效率高**：LDAP 目录服务专门针对快速响应和大容量查询等读密集型的操作进行了专门的优化，因此，可极大地提高**数据读取和查询性能。**
- **安全性好**：LDAP 提供很复杂的不同层次的访问控制或者 ACL，以控制对数据读和写的权限，可以根据谁访问数据、访问什么数据、数据存在

什么地方以及其它对数据进行访问控制，因这些访问可以在服务器端控制，这比用客户端的软件保证数据的安全可安全多了；此外，LDAP 服务器可以用“推”或“拉”的方法复制部分或全部数据，例如：可以把数据“推”到远程的分支机构/办公室，以增加数据的安全性。

目录服务是提高网络安全、降低网管费用、减轻工作强度的有效工具。

- **成本低**：不像很多商用的关系型数据库，不必为 LDAP 的每一个客户端连接或许可协议付费，大多数的 LDAP 服务器安装起来很简单，也容易维护和优化。复制技术是内置在 LDAP 服务器中的而且很容易配置；而如果要在 DBMS 中使用相同的复制功能，则需要支付额外的费用，而且也很难管理。

利用目录服务可以实现以下功能：

- 组织机构内部拥有内部信息资源的管理，以分布方式存储有关系统构成的信息，在多个服务器中复制目录，通过查询目录服务器来获得所需要的信息；
- 提供白页和黄页查询服务，如单位的服务电话、通信地址等；
- 实现单一用户登录，统一管理服务、资源和应用程序的使用；
- 对组织机构所提供的服务功能提供统一目录管理，便于注册、查找和修改；
- 信息资源的即时更新，使得目录访问者可以随时获得最新的信息；
- 广义的意义讲，安全证书管理、DNS、NIS、UDDI 等都可以纳入到目录服务的范畴。目前 CA 中心的安全证书管理和 UDDI 注册库的管理都使用了 LDAP 目录服务。LDAP 目录服务提供的是一种统一的目录访问的服务，其与对外所提供的服务功能是没有直接关系的，其所提供的是一种目录服务的统一机制。所以这里说的目录服务是 X.500 目录服务以及其简化版本 LDAP。

1.2.3 LDAP 目录的结构

LDAP 目录以**树状的层次结构来组织和存储数据**，目录由目录入口对象(Entry)组成，目录入口对象(Entry)相当于关系数据库中表的记录，可直接成为 LDAP 目录记录，是具有区别名 DN（Distinguished Name）的属性（Attribute）集合，DN 相当于关系数据库表中的关键字（Primary Key）；属性由属性类型（Type）和多个值（Values）组成，相当于关系数据库中的域（Field）由域名和数据类型组成，只是为了方便检索和灵活性的需要，LDAP 中的 Type 可以有多个 Value，而不是关系数据库中为降低数据的冗余性要求实现的各个域必须是不相关的。

这样，有以下好处：

- 一般按照地理位置和组织关系进行组织数据，同现实世界相一致，非常的直观；
- 有利于根据目录树的结构给予不同的员工/用户组不同的权限；
- 属性类型可以多个属性值，LDAP 目录就有很大的灵活性，不必为加入一些新的数据就重新创建表和索引；
- LDAP 把数据存放在文件中，可以使用基于索引的文件数据库，大大方便了检索，提高了检索效率；
- 有利于将某个地域/分支机构或某个部门/下属单位的用户信息定制推送到单独的用户目录服务器上，提高相关应用对用户信息的访问效率；
- 把 LDAP 存储和复制功能结合起来，可以定制目录树的结构以降低对 WAN 带宽的要求。

LDAP 目录记录的标识名(Distinguished Name，简称 DN)是用来读取单个记录，以及回溯到树的顶部。

基准 DN：

LDAP 目录树的最顶部就是根，也就是所谓的“基准 DN”。基准 DN 通常使

用下面的格式，如：o=orgname.com.cn (用组织机构的域名/Internet 地址作为基准 DN，这种格式很直观，这也是现在最常用的格式)。

在目录树中怎么组织数据：

LDAP 目录树的最顶部就是根。在根目录下，因为历史上(X.500)的原因，大多数 LDAP 目录用 OU 从逻辑上把数据分开来。

OU 表示“Organization Unit”，在 X.500 协议中是用来表示单位内部的机构部门。现在 LDAP 还保留 ou=这样的命名规则，但是扩展了分类的范围，可以分类为：ou=people, ou=groups, ou=devices，等等。更低一级的 OU 有时用来做更细的归类。例如：LDAP 目录树(不包括单独的记录)可能会是这样的：

```
o=orgname.com.cn
    ou=employees
        ou=office
        ou=hr
        ou=finance
        ou=sales
         ou=rd
    ou=groups
    ou=customers
        ou=china
        ou=asia
        ou=europe
    ou=rooms
    ou=assets-mgmt
```

单独的 LDAP 记录：

DN 是 LDAP 记录项的名字。在 LDAP 目录中的所有记录项都有一个唯一的“Distinguished Name”，也就是 DN。每一个 LDAP 记录项的 DN 是由两个部分组成的：相对 DN（RDN）和记录在 LDAP 目录中的位置。

RDN 是 DN 中与目录树的结构无关的部分。在 LDAP 目录中存储的记录项都要有一个名字，这个名字通常存在 cn（Common Name）这个属性里。在 LDAP 中存储的对象都用它们的 cn 值作为 RDN 的基础。

完整的 DN，比如，为一个员工“张三”设置一个 DN：

```
cn=zhang san, ou=employees, o=orgname.com.cn（基于姓名）
uid=szhang, ou=employees, o=orgname.com.cn（基于登录名，推荐）
```

推荐采用基于登录名的方式设置 DN，因为基于姓名这种格式有一个很明显的缺点---如果名字改变了，LDAP 的记录就要从一个 DN 转移到另一个 DN，但是，我们应该尽可能地避免改变一个记录项的 DN；而大多数单位都会给每一个员工唯一的登录名，因此用这个办法可以很好地保存员工的信息，而不用担心以后还会有一个叫“张三”的加入，或者“张三”改变了名字，也用不着改变 LDAP 记录项的 DN。

记录项：

LDAP 目录以一系列“属性对”的形式来存储记录项，每一个记录项包括属性类型和属性值（这与关系型数据库用行和列来存取数据有根本的不同）。

例如，机构单位 orgname.com.cn 的员工“张三”的 LDAP 记录。这个记录项的格式是 LDIF，用来导入和导出 LDAP 目录的记录项。

```
dn: uid=szhang, ou=employees, o=orgname.com.cn
    objectclass: person
    objectclass: organizationalPerson
    objectclass: inetOrgPerson
    objectclass: orgnamePerson
    uid: szhang
    givenname: zhang
    sn: san
    cn: Zhang San
    cn: Zhang Shan
    cn:  张三
```

```
cn: 张总
telephonenumber: 8610-82825858
roomnumber: 122G
o: orgname, Inc.
dept: sales
role: salesmanager
mailRoutingAddress: szhang@orgname.com.cn
mailhost: mail.orgname.com.cn
userpassword: {crypt}3x1231v76T89N
uidnumber: 1234
gidnumber: 1200
homedirectory: /home/szhang
loginshell: /usr/local/bin/sh
```

LDAP 目录可以定制成存储任何文本或二进制数据，到底存什么要由你自己决定。LDAP 目录用对象类型（object classes）的概念来定义运行哪一类的对象使用什么属性。在几乎所有的 LDAP 服务器中，你都要根据自己的需要扩展基本的 LDAP 目录的功能，创建新的对象类型或者扩展现存的对象类型。

属性的值在保存的时候是保留大小写的，但是在默认情况下搜索的时候是不区分大小写的。某些特殊的属性（例如，password）在搜索的时候需要区分大小写。

请注意 LDAP 目录被设计成允许某些属性有多个值，如一个员工可能拥有多个名字，可以用其任何一个名字检索都可以找到该员工的电话号码、电子邮件和办公房间号，等等；而不是在每一个属性的后面用逗号把一系列值分开。

因为用这样的方式存储数据，所以 LDAP 目录就有很大的灵活性，不必为加入一些新的数据就重新创建表和索引。更重要的是，LDAP 目录不必花费内存或硬盘空间处理“空”域，也就是说，实际上不使用可选择的域也不会花费你任何资源。

1.2.4 LDAP 目录的存储内容

LDAP 目录是有关用户、系统、分组、网络、服务和标识的集合；LDAP 目录中可以存储各种类型的数据，LDAP 对于这样存储这样的信息最为有用，也就是数据需要从不同的地点读取，但是不需要经常更新。例如，这些信息存储在 LDAP 目录中是十分有效的：

- 单位员工的人力资源数据：员工的姓名、登录名、口令、员工号、主管经理的登录名、邮件地址、等等；
- 电话号码簿和组织结构图；
- 用户、系统、分组；
- 电子邮件地址、邮件路由信息；
- 公用证书和安全密匙；
- 客户联系列表：客户的单位名称、主要联系人电话、传真和电子邮件等；
- 资产管理信息：计算机名、IP 地址、标签、型号、所在位置，等等。
- 会议室信息：会议室的名字、位置、可以坐多少人、电话号码、是否有投影机，等等；
- 计算机管理需要的信息，包括网络资源、DNS 域名系统、NIS 映射等等；
- 软件包的配置信息；
- 以及其他，如食谱信息：菜的名字、配料、烹调方法以及准备方法；
- 等等。

对于用户管理而言，LDAP 目录中存储的信息可包括：

- 用户 UserID(或 LoginID、使用者帐号)；
- 用户身份：用户角色(可以多个角色)、用户组；
- 用户名称 Name：正式名称、常用名、别名、中英文名等；
- 用户口令/密钥 Pswd(加密存储，区分大小写，禁止任何人查询，但是可以允许用户改变他或她自己的口令)；
- 认证公钥；
- 员工号、部门名称、部门号、房间号、工位号、工作岗位、职务名称、上级主管经理；

- 联系电话、手机、分机；
- 家庭联系信息：家庭住址、邮编、家庭电话、其他联系人信息；
- 电子邮件地址、邮件服务器、邮件路由地址；
- 员工计算机信息：计算机名、IP 地址、标签、型号、所在位置，等等；
- 验证用户的 LDAP 地址
- 用户在 LDAP 中的标识码-路径
- 用户其他信息等。

1.3 用户身份认证

1.3.1 认证类型

统一用户目录管理系统支持多个安全级别的身份认证方式，参与 SSO 的各个应用系统和受保护资源可以根据自身的安全需要设置安全等级，通过低级别登录的用户在访问高级别的应用时需要进行高级别的登录。身份认证方式的安全级别由低到高分别为：

- 普通口令级：用户输入用户名和口令进行身份认证；
- 动态密码级：用户使用动态密码卡来输入动态密码；
- 数字证书级：用户使用智能卡等设备通过数字证书和数字签名进行身份认证；
- 生物测量级：用户使用指纹仪、虹膜仪等生物物理测量设备进行身份认证；
- 生物测量+数字证书级：数字证书和生物测量的结合使用。

支持多种身份验证方式：支持多个生产商的动态密码卡、数字证书卡、DSA Key 和指纹仪等设备。

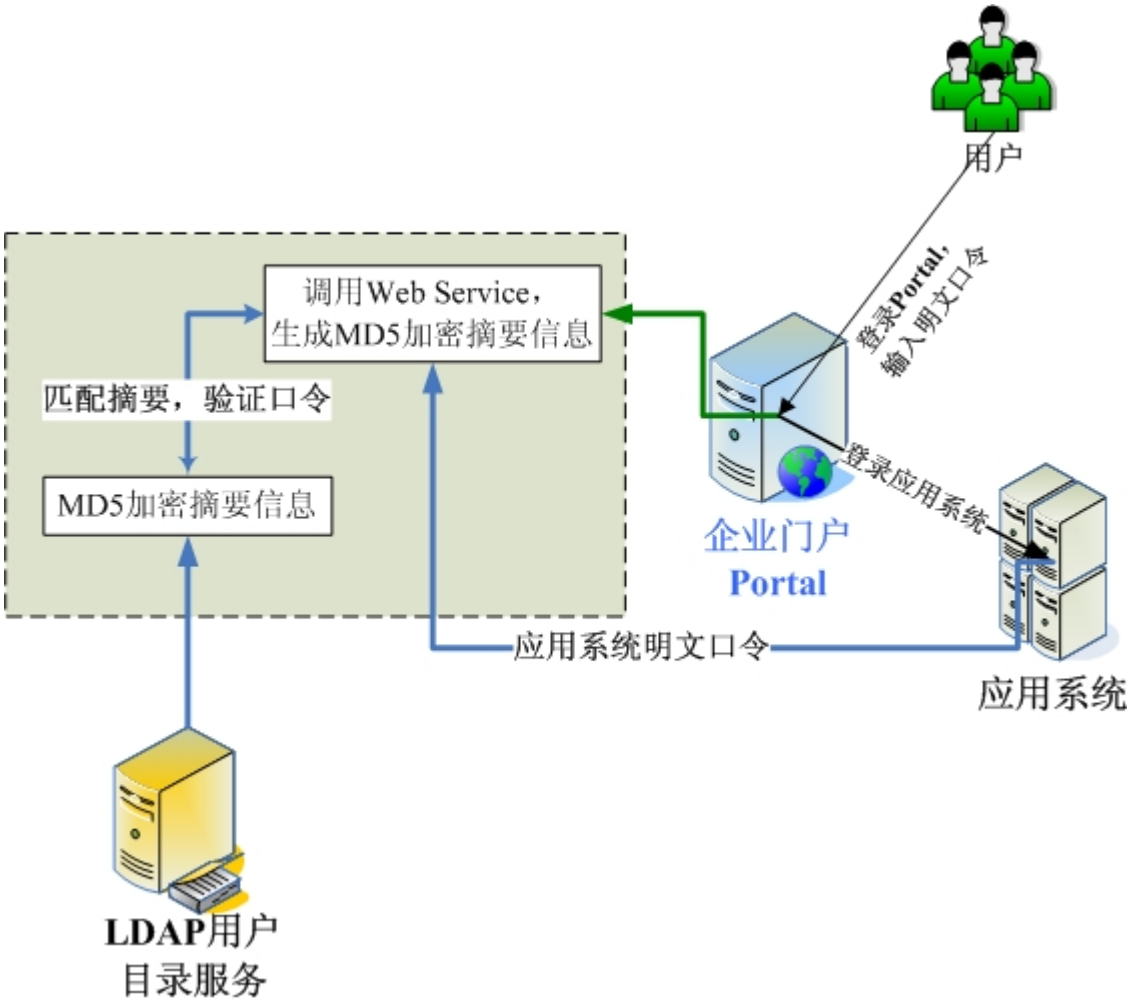
身份认证模块是以插件方式配置的，确保快速的实施和灵活的调整。

系统可以使用客户现存应用系统的已有用户数据库或 LDAP 用户目录进行身份验证；通过配置即可实现通过 LDAP 或 JDBC 进行用户身份验证。

1.3.2 用户身份密码验证

LDAP 作为存储用户信息的目录服务，可提供基本的用户身份密码验证。

为了加强用户口令信息的安全，将口令信息采用国际标准的 MD5 摘要加密算法进行摘要加密，使摘要信息可明文存储且不可逆。门户或使用该用户目录的应用系统在验证口令时，首先将用户输入的口令进行 MD5 处理，再与存储的 MD5 加密摘要信息进行匹配比较，如下图所示。



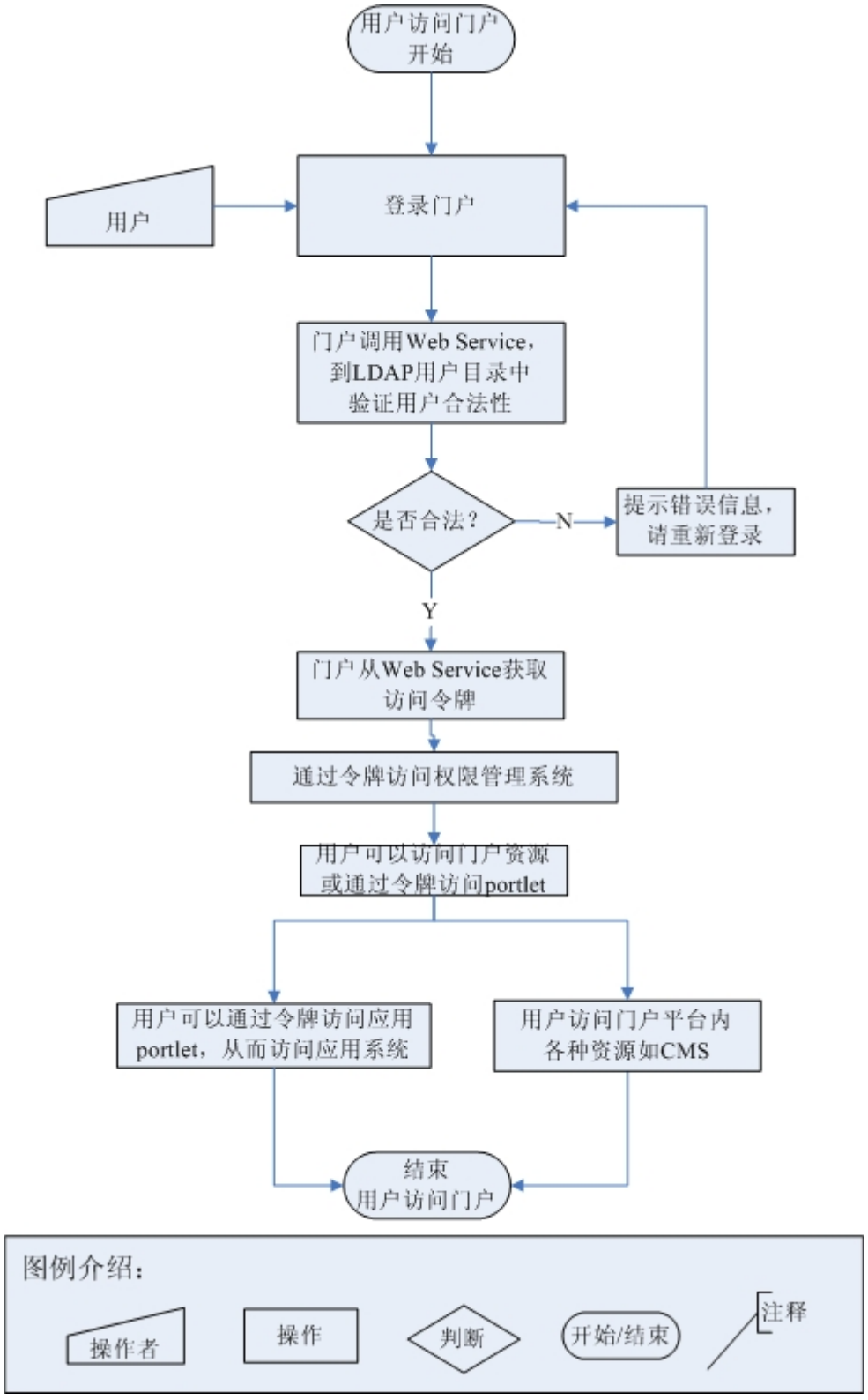
用户身份密码验证的流程如下：

（1） 用户在门户首页中输入用户名/口令，进行登录。

（2） 门户调用用户身份验证 Web Service，通过对加密后的密码摘要匹配，进行用户身份验证。

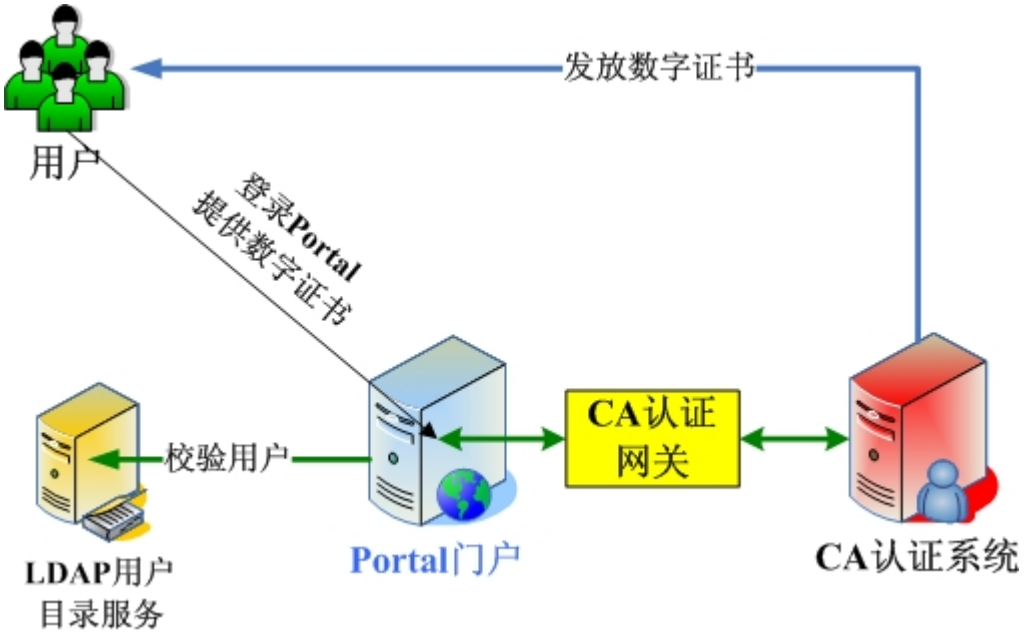
（3） 如果验证用户非法，提示错误信息并返回（1）。

（4） 用户身份验证 Web Service 返回该用户的 ID，该 ID 将作为通过门户访问应用系统的会话标识。



1.3.3 与 CA 认证接口

门户通过 CA 认证网关支持用户数字证书的验证，如下图所示；



系统提供 BJCA、协卡 SheCA、中国金融认证中心 CFCA、吉大正元 CA 等主流 CA 系统接口的支持。

1.3.4 用户登录控制

用户登录控制包括：

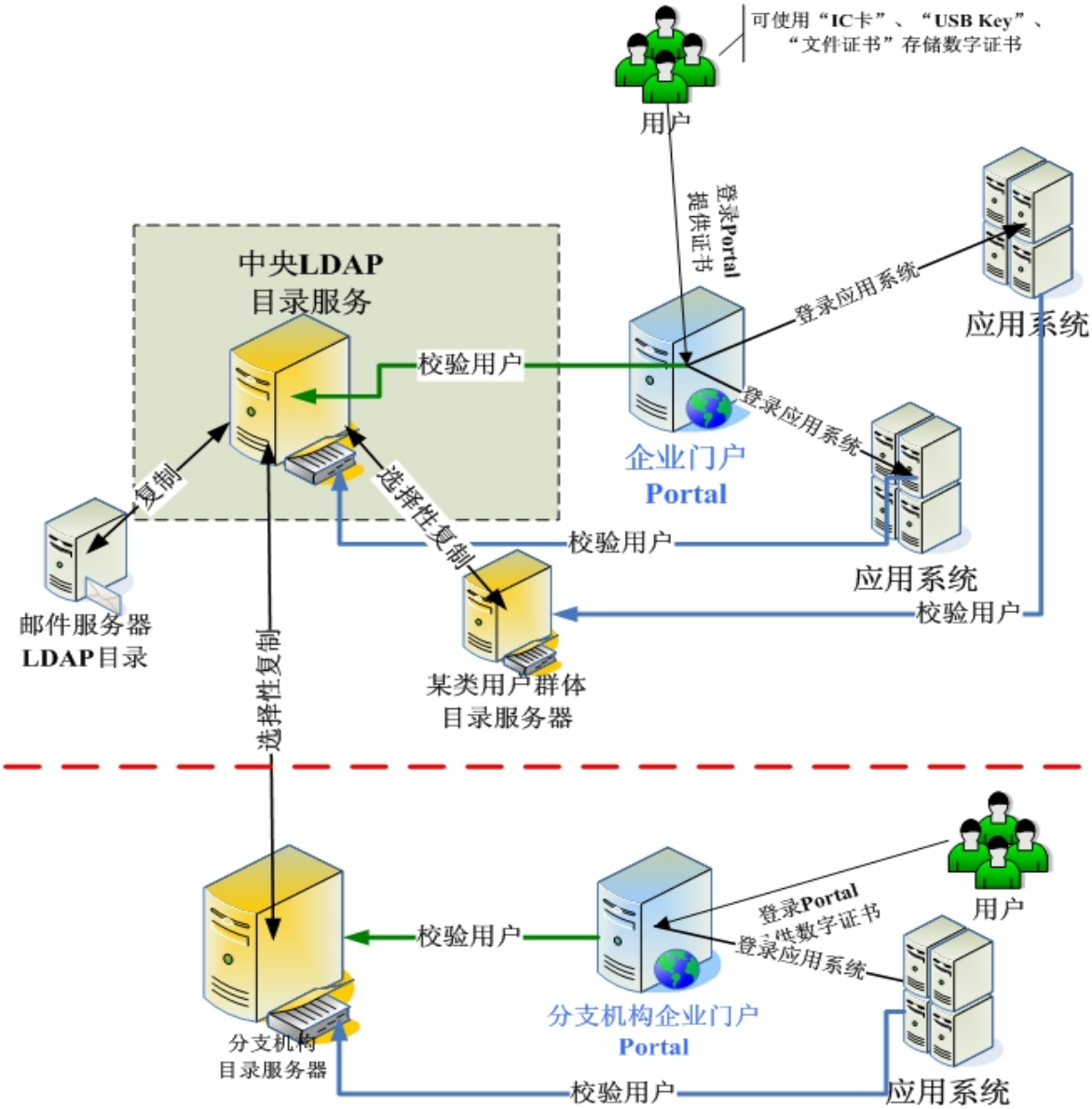
- **系统无操作时间限制**：超过 10 分钟，系统将自动退出，所有进一步操作必须重新登录。
- **IP 限制**：登录 IP 限制（特别是管理员用户）；相同用户同时登录 IP 数限制；
- **密码错误次数限制**：密码连续输入错误次数超过比如 3 次或累计次数超过比如 6 次，强制退出，不允许登录，直至系统管理员为直重置密码；
- **强制口令修改**：
  - 第一次登录时强制口令修改；

- 用户口令被重置后登录时强制口令修改；
- 口令期限：超期口令强制口令修改。

1.4 分布式用户目录管理

1.4.1 分布式目录服务体系

分布式目录服务体系如下图所示。



可配置集中目录，将所有员工信息保存到一台中央目录服务器上。中央目录

信息可以向所有用户和所有应用提供，为所有用户和组信息提供单个身份认证中心。集中目录服务可提供更多的控制，可以降低开销，并可以易于管理，具有较大的优势。

可创建多机构目录，确保用户只能访问到其所属机构的信息，如针对某个下属单位，可创建该下属单位的目录服务；再如，针对大学，可专门创建可允许学生访问的目录服务。中央目录服务器与某类用户/下属单位/部门/分支机构/远程办公室子目录服务器之间可进行选择性复制，可节约磁盘空间和复制周期。

1.4.2 目录复制

复制技术是内置在 LDAP 目录服务器中的而且很容易配置。

LDAP 服务器可以使用基于“推”或者“拉”的技术，用简单或基于安全证书的安全验证，复制一部分或者所有的数据。

例如：可以把数据“推”到远程的上海的办公室，可以建立从中央 LDAP 服务器 ldap.orgname.com.cn:1389 到 sh-ldap.orgname.com.cn:389 的有选择的数据复制，不复制需要隐藏的信息，像下面这样：

```
periodic pull: ou=northchina,ou=customers,o=sendmail.com
periodic pull: ou=hk,ou=customers,o=sendmail.com
immediate push: ou=eastchina,ou=customers,o=sendmail.com
```

“拉”连接每 15 分钟同步一次，在上面假定的情况下足够了。为了保持数据始终是最新的，主目录服务器被设置成即时“推”同步。“推”连接保证任何华东的联系信息发生了变化就立即被“推”到上海。

用上面的复制模式，用户为了访问数据只需简单地连接到本地服务器。如果改变了数据，本地的 LDAP 服务器就会把这些变化传到主 LDAP 服务器，以保持数据的同步。这对本地的用户有很大的好处，因为所有的查询（大多数是读）都在本地的服务器上进行，速度非常快。

当需要改变信息的时候，最终用户不需要重新配置客户端的软件，因为 LDAP 目录服务器为他们完成了所有的数据交换工作。

我们**推荐中央主 LDAP 目录服务器与子 LDAP 目录服务器选用同一目录服**

务产品。

不同目录服务器之间的数据移植和同步：

对于中央主 LDAP 目录服务器与子 LDAP 目录服务器选用不同厂商的产品时，首先可考虑将原有的 LDAP 目录服务器的数据移植到新的 LDAP 目录服务器中；

此外，目前，有些不同厂商的 LDAP 目录服务器之间也可以实现目录同步和复制。比如，若您正在使用 Windows 2000，可在 Domino LDAP 目录与 MS 活动目录 AD 之间同步管理用户和分组；如在活动目录中执行此操作，ADSync 允许您注册、同步属性和口令、重命名和删除 Domino LDAP 目录中的用户和分组。

1.5 统一用户信息的方式分类

门户基础平台建立一个中央统一用户目录管理系统，并支持所有应用的合法性访问。

有两种方法可以完成所有应用的统一用户目录管理。

- 第一种：**完全重新定制应用**，改变应用自身的用户体系为中央统一用户管理系统。
- 第二种：**用户信息同步**：在应用的用户管理系统与中央统一用户管理系统之间，建立用户 / 用户组同步复制关系。即在统一用户管理系统中发生任何变更，则及时反映到应用用户管理系统。（同步更新用户数据）

第一种方法可以获得最大的灵活性，但是由于要对应用系统的用户认证进行变更，工作量较大。并且仅适用于应用系统提供用户管理系统接口的前提下。

第二种方法优点在于开发较为便捷，但在后期的实际运行过程中，由于用户信息的频繁更新，有可能造成系统实际运行过程中的效率低下。

在应用系统提供用户管理接口的前提下，建议采用第一种方法：基于 LDAP 目录实现统一用户目录管理。

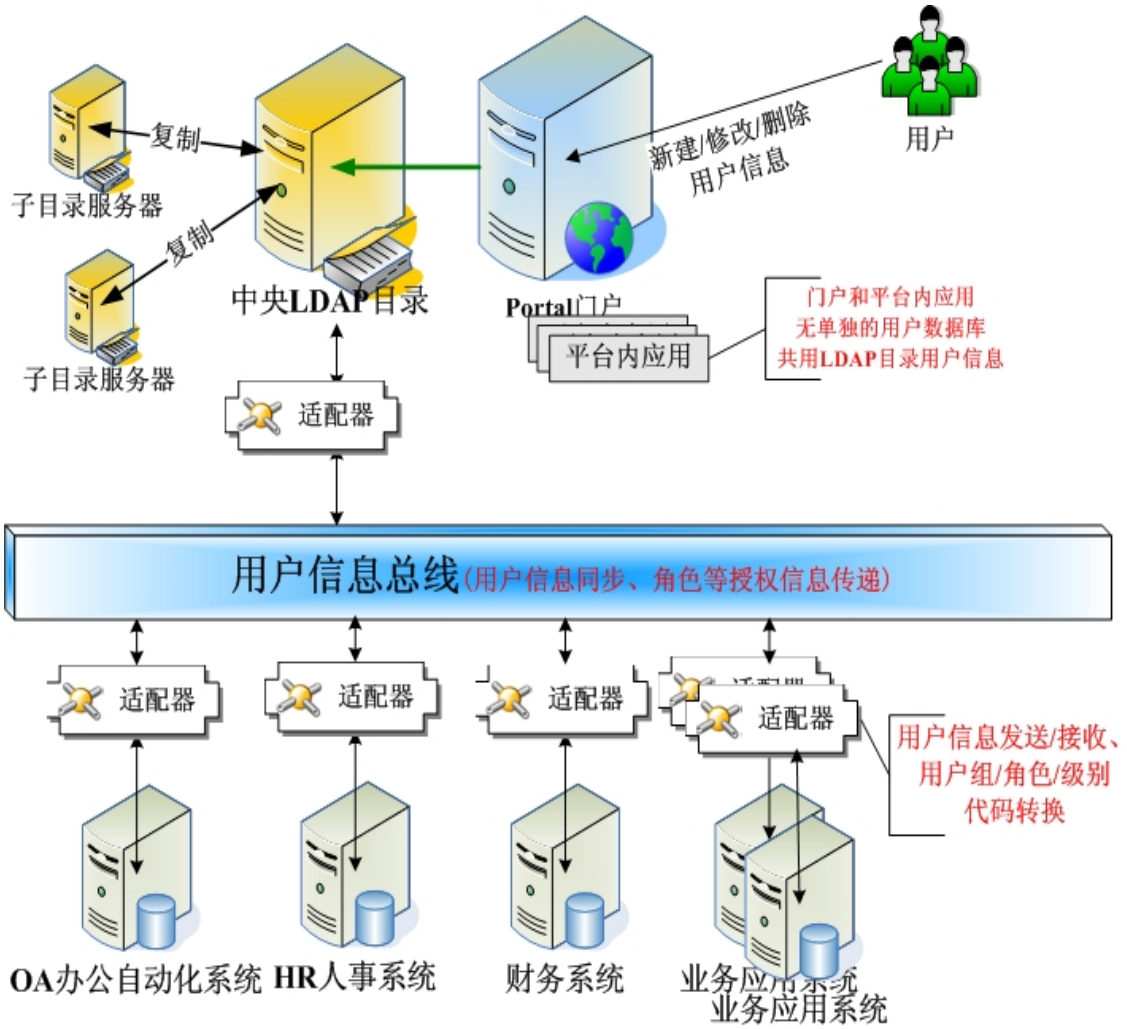
1.6 用户信息同步

随着信息技术和网络技术在组织机构中的广泛应用，很多机构单位已经拥有了各种各样的应用系统，如 OA 办公自动化系统、HR 人力资源管理系统、财务系统、CRM 客户关系管理系统、企业 ERP 系统、政府网上审批系统、学校一卡通系统、以及各种业务应用系统。

而通常情况下，各个应用系统都存在自己独立的用户信息数据库和授权管理机制，故而如何实现中央用户目录数据、门户用户数据与各应用系统用户数据之间的同步是信息化建设面临的重要挑战之一。

基于用户信息同步技术，只需在单点进行增加新用户、修改用户信息、或者删除老用户，其他相关应用系统的用户信息和基于用户角色等的用户授权信息都能同步发生变化，并且能够立即生效，从而简化了用户管理工作，避免了安全隐患的发生。

中央用户目录、门户与各应用系统之间的用户信息交换体系架构如下图所示。



用户信息总线是基于 EAI 技术的数据总线技术，支持用户信息数据的发布/订阅、请求/应答模式；发布/订阅通信模式完全是一种“推”（Push）的技术；而请求/应答通信模式是对传统 Client/Server 通信模式的支持，即支持“拉”（Pull）技术；可以根据具体应用的信息处理流程来选择合适的通信模式。

用户信息总线提供灵活可扩展的适配器框架结构，支持应用系统的动态加入或卸载，只需编写或定制该应用系统相应的适配器即可，即插即用。

应用系统适配器用来完成用户信息的基于 XML 标准的封装和解析、发送和接收；同时，**实现中央 LDAP 用户目录与应用系统之间用户组、角色、级别等同一语义不同数据格式的转换。**这样，对于基于用户**角色、用户组、级别**等对用户进行授权控制的应用系统而言，在实现用户信息同步的同时，实现了授权信息的传递。

此外，对于门户和平台的应用功能如 CMS 内容管理等，无单独的用户信息

存储，而直接使用 LDAP 用户目录数据，无需参与用户信息交换。

1.7 用户生命周期管理

1.7.1 新建用户

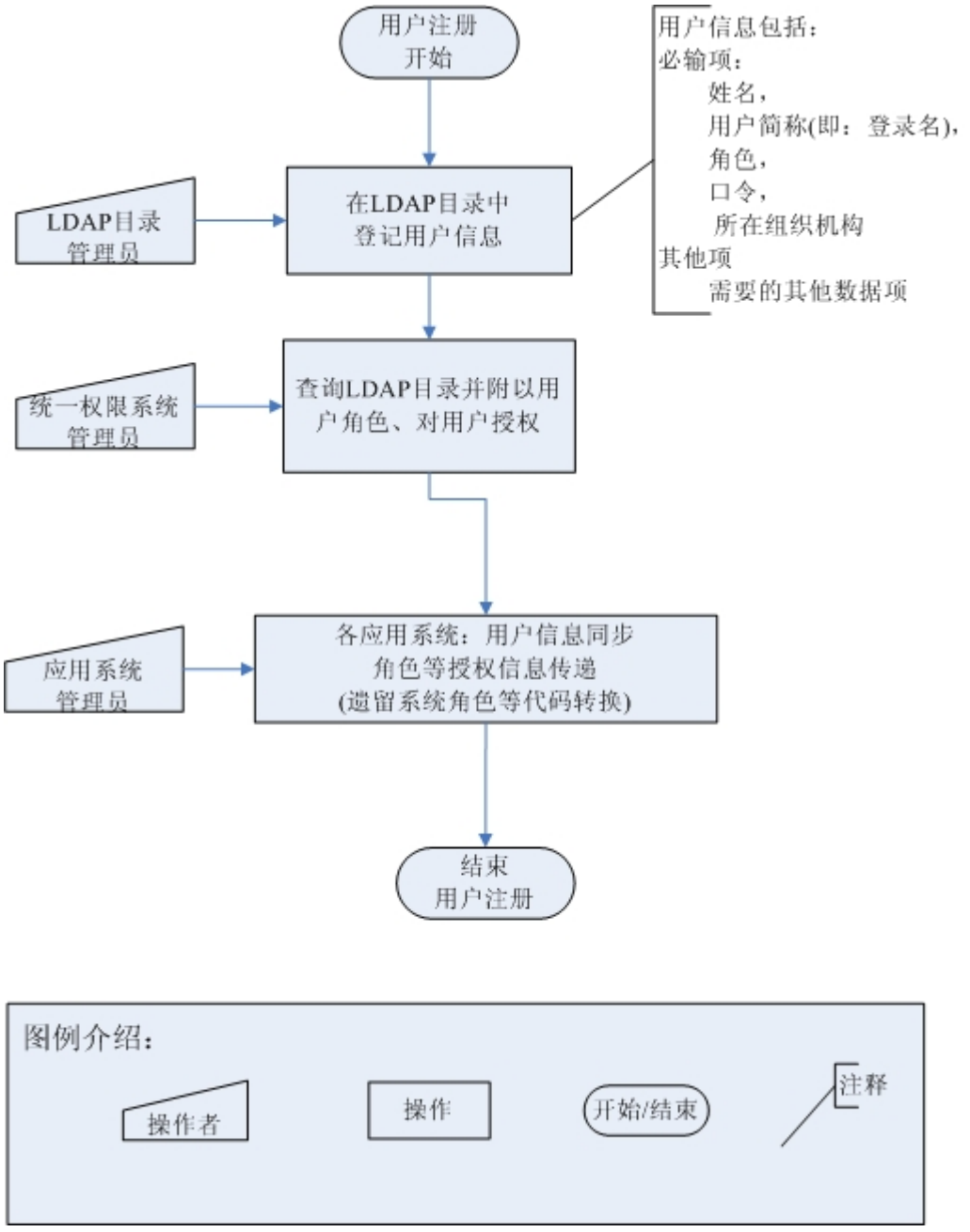
如果有新员工加入，系统提供通过 LDAP 目录管理工具登记注册新用户；同时，通过用户信息同步和授权信息传递，系统自动在与其相关的每个应用系统中增加一套用户账号，并且能够立即生效，从而简化了用户管理工作，避免了安全隐患的发生。

通过 LDAP 目录管理工具登记用户基本信息，设置用户口令，并为该用户分配一个注册名。该注册名是访问应用系统的用户名，只能包含大小写英文字母和数字，并且是唯一的。建议采用用户中文名的汉语拼音作为用户的注册名。

在 LDAP 目录中新建完该用户后，该用户同时也是门户系统用户，门户用户的用户名应该与 LDAP 目录中该用户的注册名保持一致。

用户注册流程：

如果一个用户要访问门户或者应用，而 LDAP 目录中没有该用户，或者该用户在 LDAP 目录中必须的信息（如：用户简称、口令）不完整，需要按该流程进行用户注册。如下图所示。



1．若该用户信息不存在，在该 LDAP 目录中登记用户信息；并自动成为门户的用户登录信息；

2．赋予该用户用户组、角色、级别等授权信息，对用户进行授权；

3．对各应用系统的用户信息进行同步：

a) **遗留应用系统：**

i. 若在应用系统用户数据库中，该用户信息不存在，在该应用系统中新增一个用户：

1. 用户信息同步：UserID 同 LDAP 目录用户 UserID；
2. 动态随机生成一个密码，按照应用系统的规则，加密存储在应用系统用户数据库和门户用户/应用系统对照库中；
3. 用户组、角色、级别等授权信息传递；按照相应的约定规则实现用户组、角色、级别等代码的转换。

ii. 若在应用系统用户数据库中，该用户信息 UserID 已经存在，在该应用系统中更新该用户信息，但密码不变；

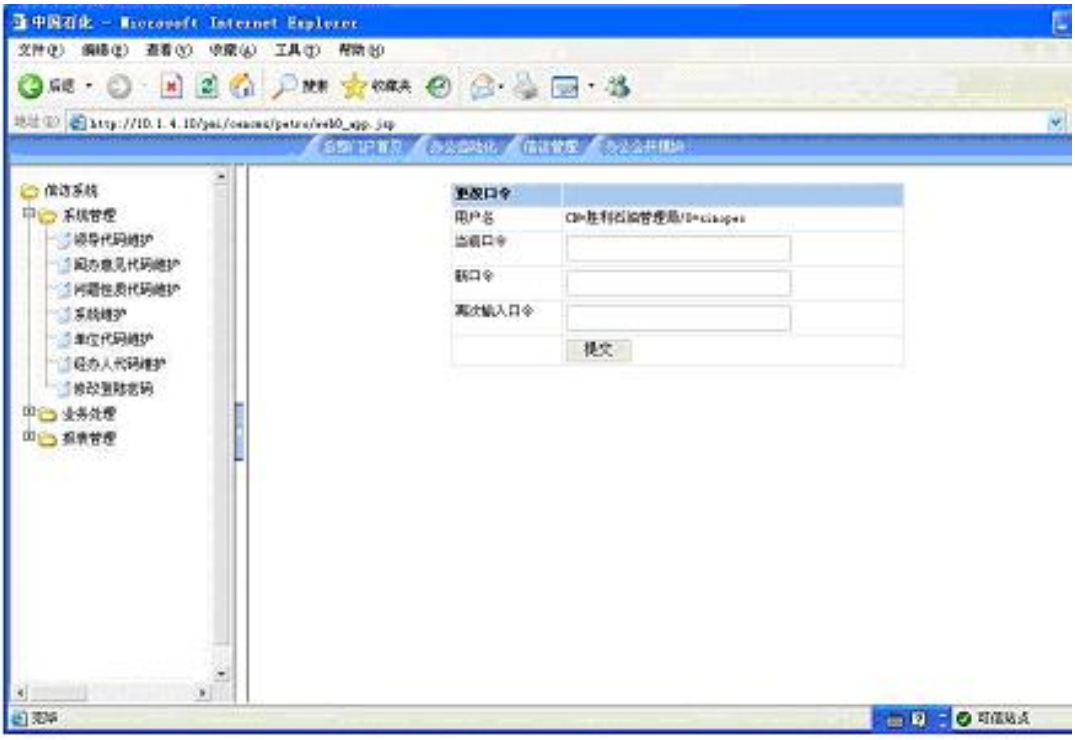
b) **新建应用系统**：

在应用系统用户数据库中新增一个用户：

4. 用户信息同步：UserID 同 LDAP 目录用户 UserID；
5. 动态随机生成一个密码，按照应用系统的规则，加密存储在应用系统用户数据库和门户用户/应用系统对照库中；
6. 用户组、角色、级别等授权信息传递(新建应用系统应遵循同 LDAP 目录采用统一的用户组、角色、级别等代码编码规则，不需要进行代码转换)。

1.7.2 密码维护

Portal 集成 LDAP 用户目录更改口令 Portlet，供用户在门户中修改口令，如下图所示。



因用户在门户中所更改的口令，即为 LDAP 目录用户口令。

对用户口令/密钥约定如下：

- 应加密存储；
- 区分大小写；
- 口令应有长度限制，如必须大于 6 位字母或数字；
- 禁止任何人查询，但是可以允许用户改变自己的口令；
- 用户第一次登录必须应强制更改口令；
- 系统管理员可重置用户的口令，但用户下次登录时应强制更改口令；
- 口令拥有有效期如 1 个月，过期后，用户登录时应强制更改口令。

对应用系统的口令更改：

对应用系统的口令更改，应通过应用系统所提供的口令更改功能，输入原口令和新口令，进行口令更改；

对于通过门户系统自动产生的对某个用户在应用系统中的口令，一般不鼓励用户用该用户名/口令直接登录该应用系统，而是应通过门户登录该应用系统；若要进行应用系统的用户口令更改，则必须经该应用系统的系统管理员对该用户

口令重置，然后，用户再进行应用系统的口令更改。

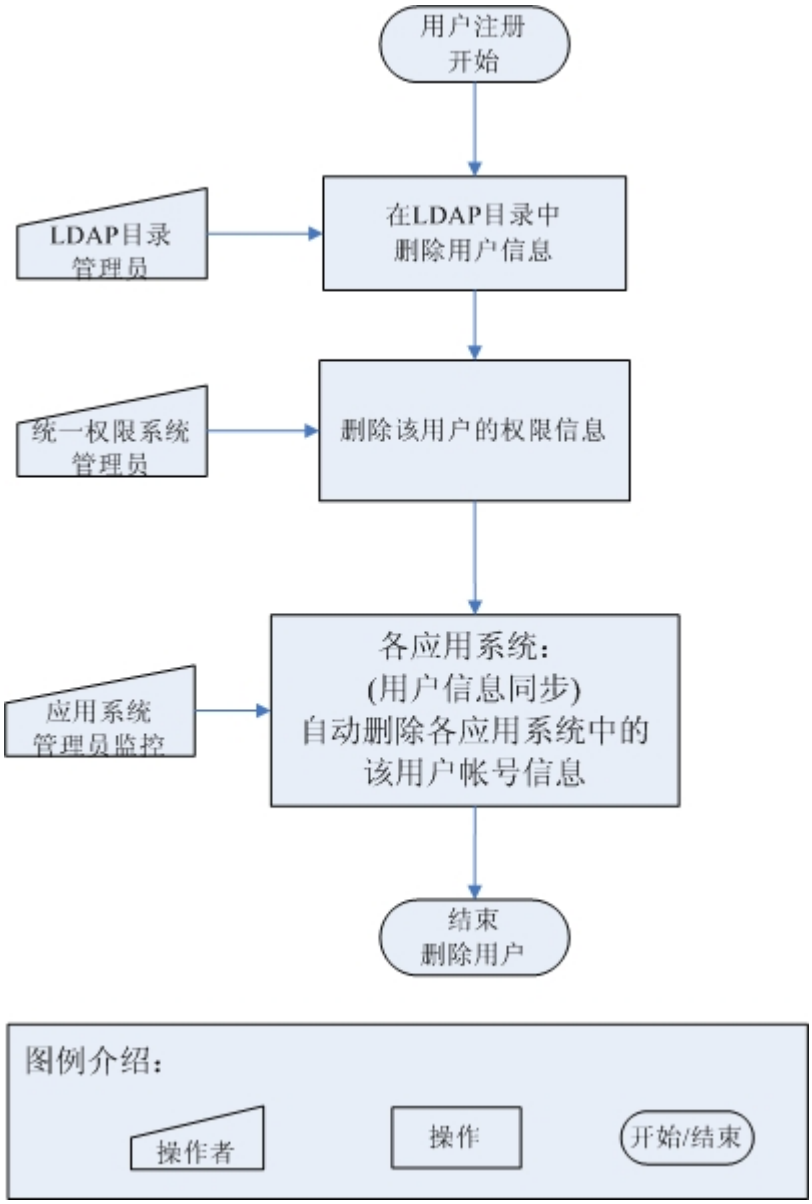
1.7.3 删除用户

如果有员工离开单位，系统提供通过 LDAP 目录管理工具删除该用户信息的同时，通过用户信息同步技术，在与其相关的每个应用系统中删除该用户的一套用户账号，从而使得删除老用户能够方便地完成，并且立即生效，从而简化了用户管理工作，避免了安全隐患的发生。

删除用户流程：

1. 在 LDAP 用户目录中删除该用户信息；
2. 删除该用户在统一权限系统中的用户信息；
3. 删除该用户在门户中的相应用户信息，如门户与应用系统之间的用户帐号映射库；
4. 基于用户信息同步技术，删除该用户在各个应用系统中的帐户信息。

如下图所示。



1.8 获取用户信息接口调用规范

根据令牌查询用户信息:

服务名: getUserInfo；

服务描述: 根据用户的令牌，查询并返回用户基本信息；

返回值：字符串：以 XML 标识的用户信息；

参数信息：令牌　字符串类型

根据用户 ID 查询用户信息：

服务名: getUserInfoByID；

服务描述: 根据用户的 ID，查询并返回用户基本信息；

返回值：字符串：以 XML 标识的用户信息；

参数信息：用户 ID　整数类型

查询用户登录信息：

服务名：getUserLoginInfo；

服务描述: 根据用户的令牌，查询并返回用户登录信息；

返回值：字符串：以 XML 标识的用户登录信息；

参数信息：令牌　字符串类型